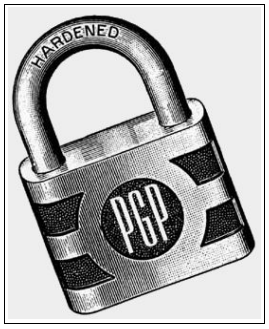
CYPHERPUNK

Criptografía rebelde.

by EVhAck

La historia de la criptografía incluye personajes tan ilustres como el poeta Edgar Alan Poe, el matemático Claude Shanon o el emperador romano Julio Cesar. Pero no será hasta la década de los 70 y el posterior advenimiento de la era Internet que un grupo de personas consiga superar los límites de la inteligencia militar y la curiosidad matemática introduciéndo la criptografía en todos los rincones de la vida cotidiana: los *cypherpunks*. Gracias a ellos podemos hoy mantener comunicaciones seguras. La historia de estos pioneros es la historia de la libertad que gozamos hoy en el ciberespacio.



"La privacidad es necesaria para una sociedad abierta en la era electrónica. La privacidad no es secretismo. Una cuestión privada es algo que no queremos que todo el mundo sepa, pero una cuestión secreta es algo que no queremos que nadie sepa. La privacidad es la capacidad de revelarse selectivamente al mundo".

ERIC HUGHES. *Un manifiesto CypherPunk*

LA HISTORIA DEL CYPHERPUNK[1] es la historia de la definición de la frontera entre lo privado y lo público, el pilar de la política telemática. En ella han participado científicos, espías, políticos, visionarios, matemáticos, empresarios y, como no, hackers. Durante los 70 y 80 unos tipos con barbas y camisetas revientan el monopolio estatal de la criptografía: creando y distribuyendo herramientas de criptografía de clave asimétrica, una garantía para la privacidad y el comercio en la red.

Estamos en los años 70 y la NSA[2] (Agencia de Seguridad Nacional) y otras agencias gubernamentales parecidas guardan celosamente todo lo que tiene que ver con la criptografía. Tienen bajo su control a la gran mayoría de científicos y matemáticos que despuntan en estas áreas, impiden la publicación de artículos criptográficos manteniendo a la sociedad civil al margen del poder de proteger sus comunicaciones. Sin embargo, nombres como Whitfield Diffie, Martin Hellman[3], Rivest, Shamir y Adlman (RSA)[4] o Phil Zimmermann[5] encabezarán la lista los luchadores contra el monopolio gubernamental de las comunicaciones

Phil Zimmermann, autor de PGP, un programa de cifrado de comunicaciones basado en la criptografía asimétrica y uno de los personajes más importantes de la escena cypherpunk. Esta foto fue realizada justo después de que Phil, en 1996, saliera airoso de uno de los tantos juicios con los que la administración norteamericana le ha presionado durante años.

seguras, creando sistemas de cifrado seguro y cambiando de forma irreversible la importancia que tiene hoy en día la criptografía para nuestras vidas en la red (y fuera de ella).

Criptografía de clave publica: el nacimiento de una amenaza para el monopolio de la NSA

David quiere mandar un mensaje a Teresa pero entre ellos no se conocen y encima saben que Pedro quiere escuchar su conversación y quiere hacerse pasar por David. ¿Cómo podría resolver este problema un sistema criptográfico? Éste fue el dilema que, durante muchos años, mantuvo a uno de los pioneros de la criptografía digital, Whitfield Diffie, recorriendo Estados Unidos en su *Dantsu 510,* en busca de una respuesta a lo que pensaba que sería la clave para las comunicaciones electrónicas del futuro. En 1970 conoce a Martin Hellman, contagiándole su entusiasmo por el tema. Ahí estaban, un ex-hacker del MIT con un profesor de Stanford unidos en la búsqueda de una solución que la criptografía de la época no parecía poder resolver.

En noviembre de 1976, Diffie y Hellman publican el artículo "Nuevas direcciones en la criptografía"[6]. Como en tantos otros casos en la historia de la ciencia y la ingeniería la solución resultó ser una idea sencilla pero tremendamente poderosa: dividir la clave en dos. David crea dos claves, una privada y otra pública, y le envia a Teresa su clave pública al tiempo que Teresa hace lo mismo. Si David quiere mandar un mensaje a Teresa debe utilizar su propia clave privada y la clave pública de ella para cifrar el mensaje. Así, Teresa es la única persona que puede descifrar el mensaje ya que ésto sólo puede hacerse combinando las dos claves inversas (la pública de David y privada de Teresa). En este caso aunque Pedro se haga con la clave pública de Teresa y con el mensaje de David, nunca podrá descifralo sin la clave privada de Teresa. Además David puede firmar su mensaje usando su clave privada, de tal modo que Teresa pueda certificar que el mensaje viene de David (y no de malicioso Pedro) combinando el mensaje cifrado de David con la clave pública de éste último.

Así, el artículo de Diffie y Hellman no sólo fue pionero en hacer uso de dos claves, sino también en romper con el secretismo de la NSA. La puerta quedaba abierta para la investigación e implementación pública, al margen del control gubernamental. Así, en 1978, se publica el algoritmo RSA, acrónimo formado con las iniciales de sus autores

1 http://www.cypherpunk.org

2 http://www.nsa.gov/

3 http://es.wikipedia.org/wiki/Diffie-Hellman

4 http://es.wikipedia.org/wiki/RSA

5 http://www.philzimmermann.com/ES/background/index.html

6 http://citeseer.ist.psu.edu/diffie76new.html

(Rivest, Shamir y Adlman) que aplicaron por primera vez, y de forma eficaz, la idea original de Diffie y Hellman. No contentos con ello, el trio de visionarios funda la empresa RSA Data Security Inc[7]. La NSA empieza a ponerse nerviosa. Durante los años siguientes, el gobierno de Estados Unidos, se adentra en una espiral de litigios y presiones para evitar la proliferación de la criptografía asimétrica. El acoso continuado a los usuarios y científicos, que utilizaban e investigaban públicamente algoritmos de cifrado efectivos, termina uniéndo a éstos y haciéndoles crear una fuerte comunidad de desarrollo y defensa de la privacidad en la red.

Logotipo pro-criptográfico de la Electronic Frontier Foundation (http://eff.org) una de las agencias independientes que con más ahínco ha defendido (y sigue defendiendo) el uso de la criptografía en la red y otros derecho digitales.

Criptoanarquía

Phil Zimmermann, activista antinuclear detenido junto a Carl Sagan en una de las múltiples protestas que protagonizaron, se reincorporó al mundo de la criptografía al conocer a Charlie Merritt, a mediados de los 80. Merritt intentaba integrar el algoritmo RSA en un microordenador, el sueño que, sin mucho éxito, había intentado realizar el propio Zimmermann en 1977. El encuentro con el atrevido Merritt lo impulsa a volver a intentarlo. De 1984 a 1991 Zimmermann se dedica exclusivamente al desarrollo del programa informático más famoso y extendido de la criptografía digital: el PGP (Pretty Good Privacy ---privacidad bastante buena). Pero es la manera en que se hizo publico el progama PGP[8] lo que lo convirtió en algo histórico para el activismo telemático.

> « Si la privacidad es declarada ilegal, sólo los ilegales disfrutarán de la privacidad »

Por aquél entonces, Joseph Biden, senador de los Estados Unidos publica el borrador 266 de la nueva ley antiterrorista, que venía a exigir a los proveedores de servicios de comunicaciones electrónicas y fabricantes de equipos electrónicos el acceso a los contenidos originales de las transmisiones (voz, datos etc.). Zimmermann se dio cuenta de que, si no lanzaba pronto su programa al mundo, la aplicación de la ley impediría. irreversiblemente, su publicación y distribución. Así que decidió, con la ayuda de los ciberactivistas Kelly Goen y Jim Warren difundir, el programa por la, por aquel entonces desconocida pero incipiente, Internet.

El primer fin de semana de junio de 1991 Goen, con un portátil, un módem y un acoplador acústico, marcha de cabina en cabina subiendo el programa a diferentes destinos de la red. Al día siguiente, personas de todo el mundo cifraban sus mensajes con PGP. Zimmerman distribuyó el programa gratuitamente garantizando además su transparecia al hacer el código accesible. Consideró más importante la privacidad que rentabilizar económicamente los 7 años de trabajo. En la propia documentación se podía leer la siguiente frase: *"Si la privacidad es declarada ilegal, sólo los ilegales disfrutarán de la privacidad"*.

En los primeros años de los 90 Eric Hughes escribiría el manifiesto cypherpunk[9] recogiendo el sentir de una comunidad que hizo y sigue haciendo posible disfrutar de un lugar seguro en el ciberespacio. Fueron tiempos donde lo público y lo privado dejaba de estar gestionado por el poder institucionalizado. La virtualidad de los nuevos mundos empezaba a ser real, Internet cada día era más grande y las comunicaciones electrónicas empezaban a ser cotidianas y seguras para aquellos preocupados por su privacidad.

Hoy podemos seguir disfrutando de un lugar seguro en las redes de comunicación pero no podemos descuidar su defensa. Desgraciadamente la empresa que (liderada por Zimmermann) actualiza las versiones de PGP ha sido comprada por otra que ha decidido cerrar su código (lo que ha provocado abandono del mítico criptoanarquista). Nos queda, sin embargo, la versión libre de PGP: el proyecto GPG[10] (GNU Privacy Guard) un programa extendido y fácilmente integrable en tu gestor de correo favorito. En nuestras manos queda hacer frente al recorte de libertades con el que bajo al excusa antiterrorista se amenaza, una vez más, la herencia de los pioneros *cypherpunk*. ✪

EvhAck
la mujer que se atrevió a morder la manzana prohibida
del conocimiento, el pecado original del hacker
(evhack.info@gmail.com)

Metainformación del Documento

VERSIÓN: versión 1.1 del Lunes 9 de Marzo del 2006

URL: http://barandiaran.net/textos/evhack/cypherpunk/

PUBLICACIÓN: Publicado originalmente en la revista ARROBA.

EXTENSION: 1373 palabras 8498 caracteres

[7] http://www.rsasecurity.com/

[8] http://www.ugr.es/~aquiran/cripto/expedien/exped002.htm

[9] http://suburbia.sindominio.net/article.php3?id_article=81

[10] http://gnupg.org